

**AFFIDAVIT IN SUPPORT OF A  
COMPLAINT AND ARREST WARRANT**

I, Edward C. Ainsworth, being duly sworn, hereby state:

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security (DHS), Immigration & Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since November 2010. I am currently assigned to the Houlton, Maine office. I have participated in numerous criminal investigations, to include matters involving the sexual exploitation of children. In my career I have utilized various investigative tools and techniques to include the use of search warrants.

2. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

3. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252A(a)(5)(B), regarding the possession of child pornography, have been committed by the defendant, Andrew LADICH-MCGREW.

**Count One: Possession of child pornography on or about June 23, 2020**

4. On June 23, 2020, members of the MCCU and HSI executed a State of Maine search warrant at 8 Strawberry Bank Road, Apartment 8 in Presque Isle, Maine. This search warrant was based on a report by electronic service provider Discord that a certain user account—later linked to Andrew Ladich-McGrew—was involved in the dissemination or

possession of sexually explicit images of children under the age of 16. Discord is an online communication platform that, among other functions, allows users to communicate with text-based chats and to send and receive media files.

5. Initially SA Ainsworth and MCCU Special Agent Armstrong met with Individual 1, the roommate of LADICH-MCGREW. Individual 1 informed investigators that he did not have a Discord account, but that LADICH-MCGREW did have one. Detective (DET) Jason Bosco and SA Ainsworth then interviewed LADICH-MCGREW outside of his residence. During the consensual interview, LADICH-MCGREW explained that he had previously saved files from an online storage drive to a drive attached to his computer. LADICH-MCGREW stated that he used multiple online Discord profiles including “PIXL01” and “Mystic Blaster.” LADICH-MCGREW stated that he had accessed the files 10 to 30 times after downloading them. LADICH-MCGREW also confirmed that he had shared 50 to 100 of the images through Discord. LADICH-MCGREW admitted to speaking with a suspected underage girl from the United Kingdom.

6. On September 24, 2020, MCCU Computer Forensic Analyst Keith Lagasse completed a forensic report of the evidence seized from the search warrant on June 23, 2020.

7. The following are findings from that examination:

- a. The following storage devices were examined: 1TB Samsung SSD (Labeled Product of Korea Manufactured December 2019), and a 2 TB Seagate FireCuda SSHD (Labeled Product of Thailand Manufactured December 2019).
- b. The following are some of the owner identifier artifacts that were found:  
“andre,” “andrew ladich mcgrew,” “ae22cb470640b2ad,” “blaster56745,”

“mysticblaste,” “mysticblaster,” “mysticblasters,” “kaiba00991,” “anderwl,” and “Seto1481.”

- c. Upon searching media files, approximately fifty-three (53) images were identified as depicting the sexual exploitation of minors ranging in age from infancy to approximately 13 years in age.
- d. Fifty-two (52) web history artifacts were recovered which suggested that the device was used to access Discord via a web browser.
- e. Further examination of the device found one hundred and nine (109) additional images depicting the sexual exploitation of minors. These images ranged in age from toddlers to approximately 13 years of age. Eleven (11) of these files were located in the unemptied recycle bin and the remaining ninety eight (98) were located under “New Volume\new folder (2)\” in various folders to include a folder named “CP Vids.”
- f. Further examination of video files resulted in three hundred and ninety-six (396) videos depicting the sexual exploitation of minors. Depicted in the videos are what appears to be prepubescent and pubescent females and males engaging in lewd/provocative poses, masturbation, bestiality, bondage, oral, anal, and vaginal sex with adults, other children and solo. All of the videos were located under file path “New Volume\new folder (2)\” in various folders to include a folder named “CP Vids.”
- g. A case referral was sent to NCMEC with the suspect files in this report. NCMEC processed this request on June 10, 2021. In their Child Recognition & Identification System (CRIS) review, they returned TA Report 140717

which identified victims by file type. The CRIS findings in TA Report 140717 included: 54 known images, 130 known videos, 2 “other files” and a total of 95 known series identified.

h. The following files will be listed as Exhibits 1 and 2 from the forensic examination:

i. Exhibit 1 is a still image from a video which depicts a girl of about 3 to 5 years of age, blindfolded, having her genital area licked by a dog. During the video, an adult hand can be seen directing the dog where to lick the child. Approximately 35 seconds into the video, yellow cordage is visible which has been used to bind the child’s legs open. The adult hand then returns to rub an unknown substance on the child’s vaginal area for the dog to consume. The camera then redirects to the face of the child where a penis can be seen inside the child’s mouth. This video was previously identified as part of an Immigration and Customs Enforcement federal investigation in another state involving a well-known series. Because I am aware through law-enforcement information that this image was produced outside the State of Maine years ago, I am able to conclude that it travelled in interstate or foreign commerce before coming into LADICH-MCGREW’s possession.

ii. Exhibit 2 is a still image from a video compilation of child sexual exploitation. The video is 8 minutes 29 seconds in length and depicts a plethora of children engaged in a myriad of sexual activity to include oral, vaginal, and anal sexual penetration. The still image is of one clip, within the montage, of an adult male penetrating the vaginal area of a small child approximately 2 to 4 years of age. This video was also previously identified as part of an Immigration and Customs Enforcement federal investigation in another state involving a well-known series. Because I am aware through law-enforcement information that this image was produced outside the State of Maine years ago, I am able to conclude that it travelled in interstate or foreign commerce before coming into LADICH-MCGREW’s possession.

**Count Two: Possession of child pornography on about October 21, 2021**

8. On November 27, 2020, HSI Houlton received an investigative referral from HSI Ottawa, Canada regarding a Discord user reported to be from Presque Isle, Maine. They had discovered the following as part of their investigation:

a. On August 25, 2020, investigators in Alberta, Canada initiated a luring investigation after it was learned that a 13-year-old female had been communicating with several online users and had sent nude images and videos of herself to these users. One of the users was identified as “mysticblaster#9416” and the communications had occurred via the social media application Discord. The victim disclosed she had sent numerous nude images and videos to mysticblaster#9416. A potential in-person meeting had also been discussed.

b. An examination of the victim’s phone resulted in the discovery of numerous nude pictures and videos the victim had self-produced. Several of the files appear to meet the statutory definition of child pornography as defined in 18 USC § 2256.

c. Alberta investigators obtained consent to assume the online identity of the minor. On several occasions between August 27, 2020 and September 16, 2020, investigators communicated with mysticblaster#9416 in an undercover capacity during which the victim's age was re-established with the user and communications of a sexual nature were continued by mysticblaster#9416. The user also stated he lives in Maine and works at Arby’s.

d. On September 17, 2020, Alberta investigators closed their investigation regarding mysticblaster#9416 due to his statement that he lives in the United States and forwarded the case to HSI Ottawa for investigation and referral to the appropriate HSI office.

e. On November 4, 2020, HSI Ottawa served a Department of Homeland Security (DHS) Summons on Discord requesting basic subscriber information and internet protocol (IP) logs for the mysticblaster#9416 user account.

f. Discord provided the following subscriber information for the username mysticblaster#9416 that included a Google email address that contained LADICH-MCGREW’s full name and indicated that the account had been established in September 2016.

g. Discord also provided IP logs from May 24, 2020 to November 4, 2020. The two most recent IP addresses were 174.255.66.115, which is registered to Verizon Wireless, and 67.247.195.131, which is registered to Charter Communications.

h. On November 20, 2020, HSI Ottawa served a DHS Summons on Charter Communications requesting basic subscriber information for IP address 67.247.195.131.

i. Charter Communications provided the following subscriber information:

Subscriber Name: Andrew Ladich

Subscriber Address: 8 Strawberry Bank Rd., Apt. 8, Presque Isle, ME 04769

The subscriber information also included a purported Google email address similar to that recorded by Discord, but with a misspelling of LADICH-MCGREW’s name. The

provided information also included Current Lease Start of 3/24/2020 1:54:23 and Lease End of 11/24/2020 3:22:33.

9. On December 2, 2020, a preservation request was also sent to Google asking they preserve any and all records, including stored communications, currently associated with the email address from the Discord records and the email address from the Charter records for a period of 90 days. Google stated they received the request and assigned reference number 5-9527000030792 to the request. Google also advised the account associated with the email address from Charter (with LADICH-MCGREW's name misspelled) does not exist.

10. On October 21, 2021, SA Ainsworth and DET Bosco went to the residence of LADICH-MCGREW located at 8 Strawberry Bank, Apartment 8 in Presque Isle, Maine. After knocking, it took LADICH-MCGREW several minutes to come to the door. Once contact was made, SA Ainsworth explained that LADICH-MCGREW was not under arrest and asked if he would be willing to speak with the investigators. SA Ainsworth outlined the information that led investigators back to him.

11. LADICH-MCGREW explained that he did not have a phone but that he had chatted online using a homemade computer, which he constructed earlier in 2021. He said that the homemade computer, located in his bedroom, was used to chat with a suicidal girl from England, whom he thought was under age 14. He admitted to receiving the sexually explicit images from the minor and leaving them in the chat. He also said that the minor's screen name was "Kirby" and he hadn't spoken with her in a couple months. LADICH-MCGREW estimated that the total number of sexually explicit images was in the single digits. LADICH-MCGREW stated that he still was working at Arby's in Presque Isle, Maine.

12. The investigators then asked LADICH-MCGREW if he would be willing to sign a consent to search his computer. SA Ainsworth then read the electronic consent to search form to LADICH-MCGREW. LADICH-MCGREW asked to use a phone to contact his attorney prior to signing the consent form. DET Bosco called Attorney Jeremiah McIntosh, on his behalf, and informed him that the phone was on speaker mode. After speaking with his attorney, LADICH-MCGREW signed the consent to search form.

13. After the form was signed, MCCU Computer Forensic Analyst Jill Armstrong previewed his computer and identified several images of suspected child pornography. The computer was then seized and a receipt was provided to LADICH-MCGREW.

14. LADICH-MCGREW explained that the conversation with an underage female occurred on his old device which had been taken by HSI/MCCU, after the previous interview on June 23, 2020. LADICH-MCGREW explained that the minor sent him the explicit images as payment for helping her through a suicidal period.

15. When asked where he got his new CPU (Central Processing Unit), LADICH-MCGREW stated that he recently bought it new off Amazon. LADICH-MCGREW claimed that there were no images containing child pornography on his current computer. LADICH-MCGREW further stated that he was the only user of the computer.

16. When DET Bosco confronted LADICH-MCGREW about the child pornography files found on his computer, LADICH-MCGREW stated that they shouldn't be there. LADICH-MCGREW further stated that no one else used that computer and that he had not clicked on a Dropbox or Mega links containing child pornography. He confirmed that the last time we caught

him with child pornography, he had downloaded it from a Mega link but denied having gone to any since.

17. LADICH-MCGREW denied having any external drives or thumb drives that contained child pornography.

### **Initial HSI Forensics**

18. On October 28, 2021, Homeland Security Investigations (HSI) Special Agent (SA) Edward Ainsworth submitted a desktop computer to HSI SA / Computer Forensics Agent (CFA) Christopher Bennett for examination.

19. SA/CFA Bennett examined the following device:

Device Type: Desktop Computer  
Manufacturer: CyberPowerPC  
Model: C Series  
Serial Number: 16284047100570  
Installed Media: Samsung Solid State Drive (SSD)  
Media Capacity: 1 Terabyte  
Media Serial Number: S5VSNG0NA26874F  
Media Country of Origin: Korea  
Assigned Drive Letter: C:

20. Analysis of the data contained on the Samsung SSD was performed on a forensic evidence file (FEF), which is also known as a bit-for-bit copy or a forensic image, of the digital storage media, rather than the actual evidence. Performing analysis on a copy of the evidence prevents inadvertent alteration of the original evidence. In order to obtain an FEF, a device is accessed in a way that prevents alteration of the data contained on the device while the copy is created. This can be achieved using several different methods depending on the characteristics of the device being examined. Typically, the digital storage device is connected to a hardware



write-blocker, which provides write-protection during the creation of the FEF. Utilizing write-protection prevents writes to the suspect media during imaging. This process is designed to prevent alterations or modifications to the original evidence.

21. A Message Digest 5 (MD5) hash value of the original device is calculated during the imaging process and is compared to the MD5 hash value of the FEF. The MD5 hash is a 128-bit number that uniquely describes the contents of a file. The odds that two files with different contents would have the same MD5 hash value is 1 in 2 to the 128th power or approximately 1 in 340 billion billion billion billion. The MD5 hash of the original device matching the MD5 hash of the FEF confirms it is an exact copy.

22. SA/CFA Bennett used Forensic Toolkit Imager software version 4.5 in conjunction with a Tableau T35U write-blocker connected to a forensic workstation to create an FEF for the Samsung SSD. SA/CFA Bennett confirmed the MD5 hash value of the FEF matched the MD5 hash value of the original device. CFA Bennett then processed the FEF for review using Magnet Forensics' Axiom software version 5.6.

23. In the Windows operating system, the drive designated as "C: Drive" contains the operating system software and is the repository for user data and the registry. The registry is a core element of the Windows operating system as it is the repository for settings and configuration information regarding the computer system. Bennett examined the registry in the device. Basic registry information for this device included the following:

Installed Operating System (OS): Windows 10 Home version 6.3  
OS Installed/Updated Date: 1/1/2021  
Computer Name: DESKTOP-46TNFLG  
Computer Owner: blaster56745@gmail.com

User-generated Account User Name: blast  
User-generated Account Full Name: andrew ladich mcgrew  
Current time zone: Pacific Daylight Time (PDT)

24. SA/CFA Bennett noted the side panel of the computer was missing at the time of examination. Bennett's electronic forensic examination also revealed that an additional storage drive appears to have been connected to this computer prior to the time agents interviewed LADICH-MCGREW on October 21, 2021. Registry logs show that a Western Digital model WD10EZEX-08WN4A0 one terabyte hard disk drive (HDD) was initially connected to the computer on January 31, 2021 and was last removed from the computer on October 21, 2021, at approximately 7:31 am PDT, which was 10:31 am Eastern Daylight Time (EDT). SA Ainsworth stated investigators initiated an interview with LADICH-MCGREW at approximately 10:33 am on the morning of October 21, 2021 and subsequently detained the computer for examination.

25. At the time LADICH-MCGREW consented to a forensic preview of his computer during the interview on October 21, 2021, Maine Computer Crimes Unit Computer Forensic Analyst Jill Armstrong conducted an on-site preview of the computer. SA/CFA Bennett reviewed the report generated by Armstrong and found that only two drives were connected to the computer at the time of Armstrong's on-scene examination; a drive listed as the C: drive with volume serial number F4465896, which is the volume serial number of the Samsung SSD, and the government owned device Armstrong was using to preview the computer.

26. Many of the artifacts of interest Bennett identified in his examination (items listed below) reference files stored on the "D: drive." In the Windows operating system, drives are assigned letter designators in the order in which they are connected. The drive containing the operating system is assigned the designator "C: Drive," and additional drives connected will be

assigned designators starting with “D:Drive.” Since registry logs show only the Samsung SSD and the Western Digital HDD connected to the computer prior to the arrival of the investigators on October 21, 2021, the Western Digital hard drive must have been assigned drive letter “D” at the time of its removal.<sup>1</sup> This drive was not connected to the computer at the time of examination and therefore it was not examined. The Samsung SSD was the only drive in the computer at the time of examination.

27. The following information was noted and bookmarked during the subsequent forensic review of the Samsung SSD, its registry information, and associated user data:

- 51 photographic files depicting suspected child pornography. Many of the images depict children engaged in sexual acts with adults. Some of the children appear to be toddlers. All of the images are located in Windows Explorer thumbcache, which is used to store thumbnail images for Windows Explorer's thumbnail view. This speeds up the display of images as these smaller images do not need to be recalculated every time the user views the folder. Three of these images are attached to this affidavit, under seal, as exhibits:
  - Exhibit 3 depicts a girl of about 3 to 5 years of age, apparently nude, holding the penis of an adult male toward her mouth. The penis and her hand have what appears to be ejaculate on them. The girl's age is estimated from her facial features and proportions, the proportions of her arm and hand, and the relative size of the adult male.
  - Exhibit 4 depicts a prepubescent female of about 4 to 6 years of age. She is reclining on top of an adult whose is mostly obscured in the frame by the child. The child's legs are spread apart making her genitals the focal point of the image. The adult is holding up one of the child's legs; the adult appears to have painted nails. The child is holding her other leg at the knee. A small rod or pen appears to be penetrating the child's anus. The child's age is estimated from her facial features, her proportions, especial at the limbs, and the appearance of the genitals, which are devoid of secondary sexual characteristics. Breast development is not visible because the child's left arm is lying across her chest.

---

<sup>1</sup> At the time CFA Armstrong conducted her on-scene forensic examination, the government forensic drive was the second of two drives then connected to the computer, so that government drive was Designated as the D:Drive at the time of her examination.

- 56 photographic files depicting child erotica or age difficult child pornography. 55 images are located in Windows Explorer thumbcache. 1 image is in the Firefox web browser cache.
- 160 animated depictions of child pornography. 157 images are located in Windows Explorer thumbcache. 3 images were in the Firefox web browser cache.
- Numerous file artifacts with titles indicative of child pornography were located. These files include the following:
  - 256 Jump Lists, which are created by Windows and show lists of recent applications or files that a user launched.
  - 134 LNK or Link Files, which are created by Windows when a user opens a local or remote file or document. This file path shows where the opened file was stored at the time it was accessed.
  - 50 MRU or Most Recently Used Files, which are logs of files recently opened, saved, or accessed.
  - 1 Prefetch File, which is a file used to speed-up access to certain program information.
  - 12 Shellbag Files, which are files related to user preferences and appearance of Windows icons.
  - 29 Windows file history artifacts, which are created when a user accesses a file.

28. Some example file titles include the following:

- 10yo getting ass fucked.mp4
- (pthc) NEW 2016 Pedo Childlover 8yo Daddys Little Girl JM 01\_x264.mp4
- 10yo getting fingered\_mpeg4.mp4

29. Multiple artifacts suggest that a user accessed two files on the D: drive with titles indicative of child pornography shortly after midnight on the morning of October 21, 2021:

- (sdpa) vanesa 10 años cojida por el culo.3gp
- CP niña rubia se masturba.mp4

30. Google translate shows the Spanish to English translation for these files as, "(sdpa) vanesa 10 years old fucked in the ass.3gp" and "CP blonde girl masturbates.mp4." The files were accessed on October 20, 2021, at approximately 9:23 and 9:28 pm PDT, which was October 21, 2021, at approximately 12:23 and 12:28 am EDT.

31. LADICH-MCGREW previously claimed to have saved files containing child pornography on an external drive during his original interview on June 23, 2020. A forensic review of a hard drive seized on June 23, 2020 confirmed that LADICH-MCGREW had indeed stored a sizable quantity of child pornography on that hard drive. Based on the findings of the Computer Forensic Agent for the computer seized on October 21, 2021, an external drive containing images of child pornography was removed from LADICH-MCGREW's computer minutes before LADICH-MCGREW spoke with investigators on that date. LADICH-MCGREW denied having such a storage device when questioned by investigators on October 21, 2021, which was in contrast to the forensic findings.

32. Based on the fact that LADICH-MCGREW has shown a pattern of saving files containing child pornography onto storage devices and that he removed the Western Digital hard drive containing child pornography minutes before speaking with investigators, I have probable cause to believe and I do believe that that the crime of possessing child pornography occurred up to and on October 21, 2021. Further, the forensic evidence in this case indicates that LADICH-MCGREW likely removed the Western Digital drive from his computer when agents came to his home, and thereby continued to possess subject files on this drive even after his computer was taken. In order for a previously identified child pornography video to be on a computer in Maine, particularly on a computer connected to a file sharing network, it is highly likely that the video had previously been transported, distributed and received in interstate and foreign commerce. Additionally, the Western Digital Drive is known to be manufactured outside the State of Maine.


## **CONCLUSION**

By examining the evidence gathered during the search warrant and the statements made during the interview on June 23, 2020, I conclude that Andrew LADICH-MCGREW knowingly possessed child pornography on his computer. He identified during the interview that the files would be found on the drive that was removed from the residence. Furthermore, the drives containing the child pornographic material were stamped as manufactured outside of the United States and some of the files identified as child pornography were previously identified from federal investigations in states other than Maine.

By examining the evidence gathered during the consent search and the statements made during the interview on October 21, 2021, I conclude that Andrew LADICH-MCGREW again knowingly possessed child pornography on his computer. Forensic examination of his device showed that LADICH-MCGREW accessed multiple files with titles consistent with contents of child pornography within 24 hours of the interview and that the hard drive containing those images appears to have been removed minutes before speaking with investigators. Thumbnail images tied to that missing drive showed images of child pornography, consistent with child pornography having been viewed on the computer. LADICH-MCGREW stated that he was the sole user and owner of the computer seized on that day.

The above facts, in the affidavit, establish probable cause to believe that on or about June 23, 2020 and October 21, 2021 Andrew LADICH-MCGREW possessed child pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B). Exhibits 1, 2, 3, and 4 pertain to this violation.

I, Edward C. Ainsworth, hereby swear under oath that the information set forth in this affidavit is true and correct to the best of my knowledge, information, and belief, and that I make this oath under pains and penalties of perjury.


  
Edward C. Ainsworth, Special Agent  
Homeland Security Investigations

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedure

Date: Jun 01 2022

City and state: Bangor, ME



  
Judge's signature  
John C. Nilsson U.S. Magistrate Judge  
Printed name and title